AD NUMBER

ADB165821

LIMITATION CHANGES

TO:

Approved for public release; distribution is unlimited.

FROM:

Distribution authorized to DoD only; Administrative/Operational Use; APR 1991. Other requests shall be referred to National Defense Univ., Ft. McNair, Washington, DC 20319.

AUTHORITY

NDU/NWC C5/PAO 1993

1991
Executive Research Project
S54

Crisis/Emergency Management -- A Role for the Chief Information Officer

William S. Prusch
Federal Emergency Management Agency

Faculty Research Advisor
Dr. Robert E. Neilson

The Industrial College of the Armed Forces
National Defense University
Fort McNair, Washington, D.C. 20319-6000

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS Administrative or Operational Use 6 AUG 1992
2a. SECURITY CLASSIFICATION AUTHORITY N/A	3. DISTRIBUTION / AVAILABILITY OF REPORT Distribution limited to Department of Defense. All other requests should be forwarded through the National Defense University, ATTN: NDU-LD-SCH, Washington, D C. 20319-6000. Contractor's requests must be signed by their DoD contract monitor to verify "need-to-know."
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE N/A	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) NDU-ICAF-91- S54	5. MONITORING ORGANIZATION REPORT NUMBER(S) N/A
6a. NAME OF PERFORMING ORGANIZATION Industrial College of the Armed Forces 6b. OFFICE SYMBOL (If applicable) ICAF-AR	7a. NAME OF MONITORING ORGANIZATION National Defense University
6c. ADDRESS (City, State, and ZIP Code) Fort McNair Washington, D.C. 20319-6000	7b. ADDRESS (City, State, and ZIP Code) NDU-LD-SCH Ft. McNair Washington, D.C. 20319-6000
8a. NAME OF FUNDING / SPONSORING ORGANIZATION N/A 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER N/A
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) Crisis/Emergency Management--A Role for the Chief Information Officer	
12. PERSONAL AUTHOR(S) William S. Prusch	
13a. TYPE OF REPORT Research 13b. TIME COVERED FROM Aug 90 TO Apr 91	14. DATE OF REPORT (Year, Month, Day) 1991 April 15. PAGE COUNT 66
16. SUPPLEMENTARY NOTATION	
17. COSATI CODES FIELD / GROUP / SUB-GROUP	18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
19. ABSTRACT (Continue on reverse if necessary and identify by block number) See Attached	
20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Susan Lemke or Tina Lavato	22b. TELEPHONE (Include Area Code) (202) 287-9458 22c. OFFICE SYMBOL NDU-LD-SCH

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

ABSTRACT

This paper identifies three major roles for the Chief Information Officer (CIO) for improving crisis/emergency management response -- especially in the environment of the 21st Century where response to situational complexities will place increased emphasis on knowledge-based information system solutions. The three roles identified are: (1) the CIO and corporate information management (CIM), (2) the CIO and information systems management, and (3) the CIO and crisis/emergency management.

1991
Executive Research Project
S54

Crisis/Emergency Management -- A Role for the Chief Information Officer

William S. Prusch
Federal Emergency Management Agency

Faculty Research Advisor
Dr. Robert E. Neilson

The Industrial College of the Armed Forces
National Defense University
Fort McNair, Washington, D.C. 20319-6000

DISCLAIMER - ABSTAINER

This research report represents the views of the author and does not necessarily reflect the official opinion of the Industrial College of the Armed Forces, the National Defense University, or the Department of Defense.

ABSTRACT

This paper identifies three major roles for the Chief Information Officer (CIO) for improving crisis/emergency management response -- especially in the environment of the 21st Century where response to situational complexities will place increased emphasis on knowledge-based information system solutions. The three roles identified are: (1) the CIO and corporate information management (CIM), (2) the CIO and information systems management, and (3) the CIO and crisis/emergency management.

PREFACE

I have worked for the Federal Emergency Management Agency (FEMA) and its predecessor agencies for almost 30 years. There are many good reasons for working for FEMA for so long. It has an important mission. It has great people who work very hard. It has given me the opportunity to be practical in re-engineering old systems and, when necessary, to be at the forefront in the introduction of new technology. It has given me a variety of challenging and rewarding experiences in: both fixed and mobile information systems; both computer and communications technologies; and, both supervision and management roles. Obviously, FEMA has been a great place for me to work and grow!

I have agonized over this paper many long hours -- not over the content so much as over the presentation technique. In appreciation for all that FEMA has given me, I want to tell everyone of the tremendous accomplishments of a small Federal Agency of silent heroes who have done so much with so little. My dilemma is how to present the backgroud for my thesis in the form of a problem statement without seeming unappreciative or disloyal to FEMA by presenting the agency in a negative context.

I want to be viewed as an agent for the changes that will improve national emergency management -- a part of FEMA's rise to preeminence in the emergency management community and the public's eye. Therefore, please view any problems I attribute to FEMA in the academic context of setting the basis for the application and extension of promising new techniques to the

management of any information resource-dependent organization. Most of the problems I raise are endemic to most organizations including those in the emergency management community.

In this academic context, I present my perspective on the problems and challenges facing FEMA and others involved in crisis /emergency management and their supporting information systems; what techniques other organizations are using to address similar situations; and finally, how these new management techniques could be applied to improving crisis/emergency management.

This paper is presented in four chapters, culminating in a recommendation that FEMA follow a course, like most forwardlooking organizations: a course that establishes a position on the corporate board of directors for a chief information officer (CIO). It defines the roles and responsibilities for the CIO, with emphasis on:

- the CIO and information systems
- the CIO and corporate information management
- the CIO and crisis / emergency management

Chapter I discusses the "ad hoc" versus "business methods" approaches to crisis/emergency management and the consequences of each. It argues for using corporate information management techniques to refine existing and plan for future business practices.

Chapter II reviews three aspects of information resources management and information systems: the evolution of information resources management through the 1980's; corporate information management -- the concept of the 1990's; and, evolving technologies with potential application in crisis/emergency management.

Chapter III describes the roles and responsibilities of the CIO. It extrapolates a role for the CIO in crisis/emergency management from examples of successes in other information dependent environments.

Chapter IV presents my research conclusions. I conclude that substantial improvements in crisis/emergency management are possible by expanding the role of the CIO beyond the more traditional information systems management to: (1) steward of the corporate information management process; and (2) provider of responsive crisis/emergency management support services.

As mentioned earlier, it is my fervent hope that through this research I become an agent for change. I believe now is the time for change: change is necessary if FEMA is to realize the vision of its creators -- FEMA as the single point of contact in the Federal government for the full spectrum of emergency situations. Change is also necessary to realize the vision of the FEMA Director, Mr. Wallace E. Stickney -- for a national emergency management system that pools the resources of FEMA and supporting State and local governments for the protection of the civilian population.

CONTENTS

Crisis/Emergency Management --

A Role for the Chief Information Officer

"I want very much to pull together all of FEMA's resources and the resources of those who support us at the state and local levels in as integrated a fashion as possible -- to make sure that we achieve our mission of the protection of the civilian population" [1]

Chapter I: Introduction

A. Overview

Most organizations do not manage crisis and emergency situations very well! Very few take full advantage of information systems technology to facilitate crisis decision making. The media portrayals and the public perceptions of the management of most national emergencies are described with such terms as: a lack of compassion, an extremely slow response to people in dire need, and general incompetence. Even though some of these descriptions are exaggerated and sensationalized by the news media, there certainly is room for improvement.

* * * * * * * * * * * *

[1] Stickney, Wallace E. "Meet Wallace E. Stickney -- New FEMA Director" Journal of Civil Defense (American Civil Defense Association: February 1991)

B. **Purpose:**

This paper explores the role of the chief information officer (CIO) in realizing the original vision for the Federal Emergency Management Agency (FEMA) by creating an effective Federal response to national security crisis and emergency management. In keeping with the FEMA Director, Mr. Wallace E. Stickney's vision, implementation of these concepts could provide impetus for realizing an integrated national emergency management system by pooling FEMA, State, and local resources. The concepts presented here are applicable both to state and local governments and to large corporations with geographically dispersed facilities.

Specifically, this paper recommends that the FEMA, an agency which routinely deals with national security crises and domestic emergencies, exercise its original charge by taking the lead in developing the information systems framework for supporting compassionate, responsive crisis/emergency management. In fulfilling this charge, FEMA should demonstrate its suitability for this this awesome responsibility. First, it should improve the internal quality of services by establishing a forward-looking information systems organization and then, apply CIM to answer the desire of Mr. Stickney for an integrated national emergency management system.

C. Problem Definition:

FEMA is at a crossroads in its corporate life and must decide which way to go. The agency can stay the course it is on or it can leap to the forefront in national emergency management.

FEMA can continue to deliver crisis/emergency services using traditional organizational structures and methods to manage and improve its information system resources and emergency services. Having taken this approach, the Agency will find it increasingly difficult to keep abreast of challenging emergency situations and to mesh its supporting information systems with others in the emergency management community. Here we are talking about the difficulty of interfacing the disparate information systems of up to thirty-five Federal departments and agencies, territories, possessions, and fifty states.

Or FEMA can sieze on the opportunity to become the foremost agency in national emergency management by leaping forward into the information age now! FEMA can harness the power of evolving information systems by employing new organizational structures and business methods. Many forward-looking corporations have used these same techniques to successfully transform their businesses from decline into positions of leadership and strength. The application and extension of corporate information-age principles to crisis/emergency management has tremendous potential and is the subject of this research.

D. Crisis/Emergency Management

Each crisis/emergency situation is unique and dynamic. It is not reasonable to expect to use a rigid approach to emergency response. Instead, the situation dictates the use of a flexible, coordinative process to integrate people, procedures, computer hardware and software, and communications from Federal, State and local organizations. FEMA is responsible for coordinating Federal resources in national emergencies impacting the continental US.

In its role, FEMA is both an information-coordinating and information-based organization. Here, FEMA must design and implement an information systems architecture that will accomodate the various existing systems that are needed to support a response. Essentially, FEMA is an information-based organization. It uses automated information systems in each phase of the response. Therefore, information systems management and information technology are essential to the agency's mission.

Appropriately, the national decision-making process in response to national security crises and domestic emergencies reflects the management style of the President or, in the case of most disasters, his designated Federal Coordinating Official. In a similar manner, the management style of intermediary decision makers influences the process used to respond to crises by State and local governments and private industry.

In addition to the need to tailor the process to the style of the decision maker, there is a need to develop and follow a well-defined set of business methods and processes in order to be successful. Corporate Information Management (CIM) is the term being used in industry and government to describe this technique for defining business methods and processes and for making information systems an integral part of the business strategy. These CIM principles incorporate measures of performance as a means to determine where to make improvements to the methods and processes and to perfect the supporting information systems technology. The CIM principles use information systems not only as support to operations, but also to strategic advantage by offering new business alternatives.

The role of information and information technology is becoming increasingly important as crises and emergencies increase in complexity and geographic scope. There is a need for someone with the knowledge of the crisis/emergency management business, the business methods, and the information technology -- the CIO -- to work with the decision makers on the evolution of the business methods and processes -- to implement CIM. Just as American industries are finding out in their fight to stay competitive in a global environment, those in emergency management services must refine their business practices and processes in a way that capitalizes on the power of information systems.

Generally, the decision maker seeks information, intelligence, and policy recommendations from as many command and staff levels as time permits. Too often it takes too long to get an effective response organized: the crisis or emergency strikes without warning, the decision makers and their staffs may learn of the incident through the media, vital information is not available to help define the scope of the problem, and the response plan is nonexistent or outdated. Information Technology is inadequate or mis-applied. A well-honed and integrated process -- the kind that the CIO using a CIM process develops -- would bring order to this oftentimes chaotic process.

In responding to a national crisis or emergency, the evolving national security emergency preparedness (NSEP) process[2] is usually ignored in favor of the ad hoc process. Hopefully, the NSEP process will become as "the" national system instead of its current role where it seems relegated to application in some future catastrophic war-time emergency. As an important step in this process for FEMA, Mr. Stickney invoked the NSEP National Response Plan as "the" FEMA plan. Consideration should be given to using the CIO leadership concept and CIM processes in the evolution of "the" national system.

Corporations, like governments, are often not prepared for crisis either. In the EXXON Valdez Oil Catastrophe, EXXON plans were woefully out of date, some equipment needed to contain

* * * * * * * * * * * *

[2] Executive Order 12656 Assignment of Emergency Preparedness Responsibilities

the spill was disposed of for reasons of economy, and many emergency response procedures were ignored or improperly executed. Initially, when swift action could have limited damage, there was insufficient information available on which to implement a response.

Understandably, decision makers -- faced with inadequate time to acquire information -- are forced to fall back on what they are "familiar with" and "ad lib" a plan in crisis situations.[3]

The Federal and corporate responses to the EXXON Valdez oil spill of March 24, 1989 amplify the need for revamping our approach to crisis/emergency management to provide higher quality and more timely information for decision makers and respondents. By way of example, on March 31, 1989 -- a full week after the accident -- a picture on the front page of The Washington Post showed President George Bush, Secretary of Transportation, Samual Skinner, and Commandant of the Coast Guard, Paul Yost bent over a large map on the floor of the White House Oval Office reviewing the extent of the spill.[4]

* * * * * * * * * * * *

[3] Smith, Charles A.P. Decision Making Under Time Pressure: The Effects of Time Pressure on Information Search Strategy, Decision Strategy, Consistency, and Outcome Quality (University of Arizona: 1990)

[4] Mathews, Jay and Peterson, Cass "Oil Tanker Captain Fired After Failing Alcohol Test: Exxon Blames Government for Cleanup Delay" The Washington Post, pp. A1&A6 (The Washington Post Company: March 31, 1989)

It was a sad commentary to think that the President of the United States would have so little information, in so poor a form, so late after a spill. Although it was quite natural for the U.S. Coast Guard to play a key role in this incident, it was disappointing to me that FEMA did not play the leadership role in this matter. It is my thesis that FEMA will play a leadership role in future crises like this, after they have demonstrated the benefits of their application of the CIO and CIM to the spectrum of emergency management services.

By way of example of the cost impact of the lack of preparedness, a recent Washington Post article[5] put the EXXON cost of clean-up and the compensation at over $2 billion. This estimate did not include the incalculable costs to the prestige of EXXON due to their mismanagement of this situation.

The figure that follows depicts the major facets of crisis /emergency management. Literally, there are three slices to the pie which the executive must balance to manage effectively: (1) the internal management, (2) external management, and (3) propaganda. From the perspective of the EXXON chief executive officer (CEO), during the Valdez incident, he must direct the operations of his company -- both day-to-day and crisis response. He must manage externally his stockholders, officials of the State of Alaska and several Federal government agencies, etc. He must court, yet control the media.

* * * * * * * * * * * *

[5] Mathews, Jay "In Alaska, Oil Spill has lost Its Sheen" The Washington Post (The Washington Post: February 9, 1991)

A subtle second dimension to crisis/emergency management -- one that may ultimately determine the outcome of the response -- is maintenance of an overt appearance of complete control (maintain the perception of management competence) while covert actions are taken to resolve and control the unsolved problems.

Here for example, the EXXON CEO may have to present a time-phased recovery plan overtly, while covertly exploring ways to contain a massive oil spill (one larger than any contingency plan anticipated).

Contrast the sense of hopelessness surrounding the EXXON Valdez incident with the sense of control amd confidence exhibited by DOD during the Persian Gulf War. Here, DOD managed the flow of information to its advantage. It used intelligence information on the enemy's whereabouts to tactical advantage. DOD used polished press briefings and subtle control of the news media to calm the situation and to assure the American public that matters were under control. Smart weapons augmented with intelligence about the enemy, inter-unit communications, US/Allied communications were masterfully meshed to operate together. This paper and the diagram that follows envision an analgous operation in response to non-military response to crisis/emergency situations.

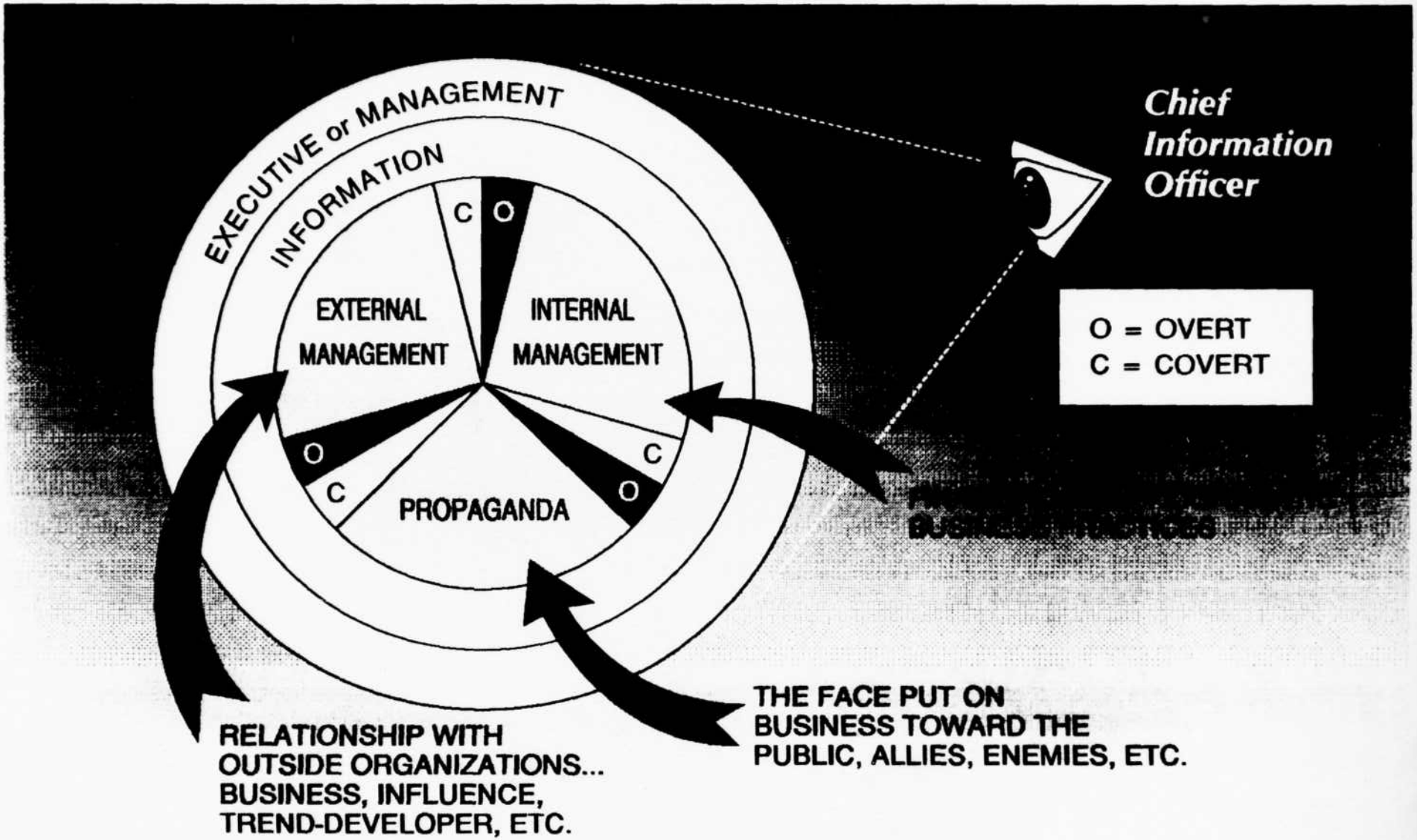

FIGURE 1. MAJOR COMPONENTS OF CRISIS/EMERGENCY MANAGEMENT

PRUSCH-91-001

Where do information systems contribute? As shown above, information systems contribute across the board -- to all phases of the decision making associated with crisis/emergency management. They do not replace management; they compliment the other contributions. They provide the means for new ways of doing business.

Where does the CIO fit into the pie? The CIO oversees, first the definition of the business methods and processes that fulfill the needs depicted by the three slices of the pie, then the refinement of the business methods and processes, and finally support using the most appropriate informations systems technology. He would ensure the proper integration of both the business methods and processes and, later, the supporting technology. Above all he would make sure the business development efforts considered the internal and external interface (the seams between the slices of the pie) issues. He would follow the CIM model in this effort.

In addressing a symposium on information technology and emergency management, Senator Albert Gore, Jr., Tennessee said,

> "Those responsible for emergency management learned long ago that their performance in times of duress often was contingent upon being able to deal with critical and useful information, which in turn was dependent upon communication between key analysts utilizing the best systems available including those drawing upon computer

and telecommunications technologies. Recent calamities such as those at Chernobyl, Mount St. Helens, or Bhopal -- with the attendant loss of life and residual property damages -- provide lessons from which we may learn. Not only must there be a preventive information network that allows advanced detection or mitigative measures to be set up, but quick reaction systems for disseminating vital data to those affected have to be in place and easily activated. In effect, I am emphasizing the importance of creating decision-making mechanisms that are equally useful in such areas of similar information collection, processing, and usage as arms control surveillance, search and rescue, weather disturbance tracking, counterterrorism, and other situations where networking of essential data is critical."

A properly designed emergency information system would have done wonders to limit the adverse consequences of this disastrous EXXON Valdez situation and would have enhanced rather than damaged the credibility of the management of both the Federal Government and Exxon Corporation.[6]

* * * * * * * * * * * *

[6] Morentz, James W. Interview with President of Research Alternatives, Inc.(Rockville, Maryland: February 4, 1991)

At the detail level there are seven major functions[7] associated with crisis and emergency management:

(1) Indication Monitoring provides the means to watch for and raise alarm levels in impending crisis or emergency situations. It also provides the mechanisms to notify higher management of the concern.

(2) Initial Crisis/Emergency Assessment is initiated when conditions warrant an increased level of monitoring and analysis. Normally, response planning is initiated. As a crisis/emergency seems more certain, an emergency response team is activated and interaction between the threat assessment and damage assessment analysts occur.

(3) Threat Assessment includes an evaluation of all possible consequences of the emerging situation. Included here are efforts to disseminate the threat assessment information to all concerned organizations.

(4) Situation/Damage Assessment are those activities designed to collect and analyze information on the scope of the crisis and the probable damage to resources. This effort is concerned with the best means to disseminate and display the information.

* * * * * * * * * * * *

[7] Phillips, Warren R. and Rimkunas, Richard Crisis Warning, pp. 2-3 (Gordon and Breach Science Publishers, New York: 1983)

(5) Resource Analysis is the computer-assisted effort to identify those resources available to effect recovery. In catastrophic emergencies the effort identifies alternative courses of action for the response planners.

(6) Response Selection/Execution is the time when the decision is made on the preferred course of action. In national security emergencies the decision may include the combining of options to one including military, economic, or diplomatic components. Of course, Response Execution is the transmission of the decision and the actual carrying out of the direction.

(7) Emergency/Crisis Monitoring is the process of ensuring that the Response Execution is effective and that the crisis is being alleviated. It feeds back to the response planning, threat assessment, and situation/damage assessment analysts.

The flow diagram that follows on the next page indicates the interaction among these seven crisis management functions.

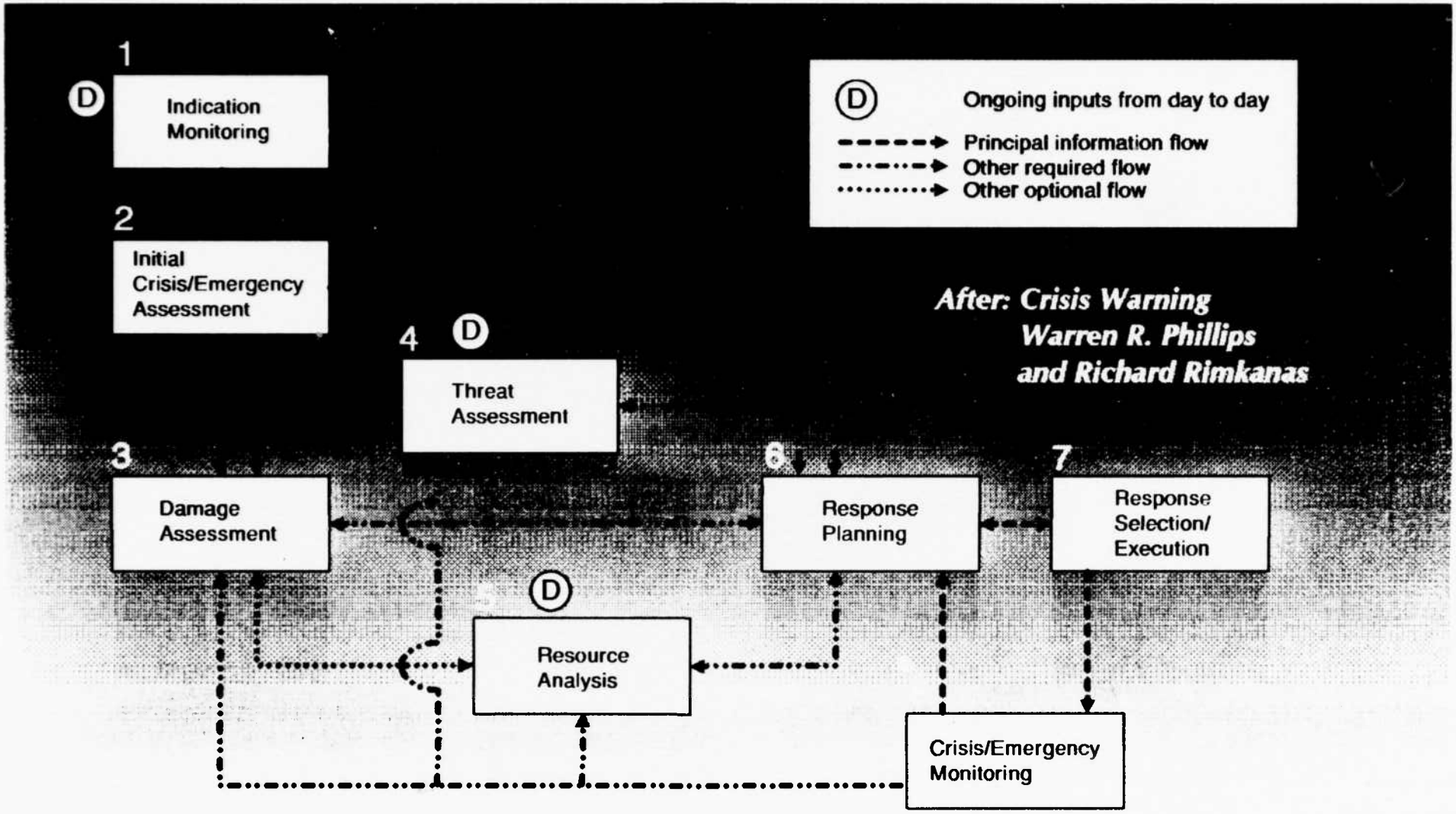

FIGURE 2. FLOW DIAGRAM CRISIS/EMERGENCY MANAGEMENT

E. Information - A Corporate Resource

In the post industrial age, information has joined labor and capital as the most important corporate resources. Alvin Toffler and other futurists see the emergence of knowledge-based societies by the 21st century where there will be an increasing cost of unreliability, of inadequate tracking and monitoring, and of late responses to demands for up-to-date information. Witness the role of information to the precision timing requirements of "just-in-time" deliveries. Information is at the core of creative thinking, which leads to new ways of doing business, new products, new procedures, new compounds, etc. -- information is used to achieve corporate goals. Information is used to gain the upper edge on the competitors by a better understanding of the customer, short circuit a manufacturing problem, or realize a technological breakthrough. As information and knowledge - based products and services become commonplace, public expectations will change. Society will expect government to use advanced technology to prevent loss of life and property and facilitate recovery. Properly applied, the CIO leadership and CIM can be the vehicles for capitalizing on the nation's crisis/emergency management resources.

Just as information is an organizational resource, it is also a national resource as indicated in the following excerpt

from Ex-President Carter's address to The White House Conference on Library and Information Services:

> "Information, like the air we breathe, is a national resource. Accurate and useful information is as necessary as oxygen to our health and happiness as individuals and as a nation. More than half of our gross national product now comes from activity related to information. Information is rapidly replacing manufactured goods as a major commodity of our economy."[8]

FEMA, by adopting the CIO and CIM principles, can make proper use of existing and evolving information systems to preserve life and to reduce the public uncertainties and anxieties that follow major crises and emergencies.

F. Information -- Its Importance to National Security

Clearly, the effectiveness with which crises and emergencies are managed depends on numerous factors, but one of the most important is the timely availability of essential information. In fact, without this crucial information, decisionmakers under duress are often paralyzed. In light of the

* * * * * * * * * * * *

[8] Carter, Jimmy "Message form the President" The White House Conference on Library and Information Service (Conference Program: November 15-19, 1979)

trends toward a global knowledge-based economy by the 21st Century and resultant complexities of life that will result, there is an increased likelihood of life and property threatening emergencies. For example, consider for a moment the potential for a crisis from the proliferation of small weapons of mass destruction.

Early recognition of a national security emergency or an international crisis, coupled with an effective diplomatic or military action can avoid an unnecessary conflict. The global intelligence information collection systems, the means to disseminate and analyze the information, and the support systems that process the information to alert and warn decision makers are of obvious importance. The failure to recognize a surprise threat could have dire consequences.

The initial crisis assessment attempts to determine whether a crisis exists or not, and if it does, the potential scope of the crisis. Reliable information is essential to this analysis. The facilities to refocus information collection and concentrate analysis contribute to the effectiveness of this step.

The availability of large stores of detailed information and of resource analysis models are crucial to the threat assessment, resource analysis and response planning activities. Information is needed to flush-out and evaluate response options.

The response selection/execution phase is heavily dependent on the availability of reliable, current, and timely information. Information is needed as input to the decision support systems that aid the response selection and to transmit the direction to those responsible for execution.

In the case where a military response is chosen, information is absolutely essential in all phases of the operation. The following are but a few of the roles for information in the execution of a military operation: target and weapons selection, transportation planning, surveillance of enemy positions, communications intercept, and bomb damage assessment. High technology (driven by embedded information systems) weaponry has been the success story of the Persian Gulf War. Information systems to distinguish friend from foe (identify friend/foe) have been one of the keys to the success of the operation of the coalition forces.

Chapter II: Information Systems Evolution

A. Evolution through the 1980's

The rapidly changing products and services of the computer and telecommunications industries have required periodic shifts in the policies and concepts for information systems management. The evolution of information resources management has occurred in stages.

The first stage in the evolution of information systems was the physical control of information: Paperwork Management. This stage began in the late 19th century and continued until the late 1950s. During this period, a typical American industry moved from a centralized, single product line organization to a geographically dispersed organization with several product lines. Government regulation, a reaction to the Great Depression, became a way of life. Information Management was a very low level service activity -- concerned with paperwork. It was usually outside the mainstream of the business.

The second stage in the evolution of information resources management spanned the 1960s and 1970s. It was characterized by the evolution of computer, telecommunications, and office automation technologies. Information resources management was aimed at enhancing the technical efficiency and physical control

of these new technologies and resources. The main focus of computer operations were on internal management information systems. During this stage, information resources activities were mid-level functions. Computer, management information systems, telecommunications and office automation functions were usually handled by separate mid-level managers.

The current stage or the traditional approach, has seen an increased convergence of the technical and functional aspects of computers, telecommunications, and office-automation technologies. The advent of integrated voice-data communications, local and wide-area networks of micro- and mini-computers, multi-function personal computer workstations which incorporate office automation and electronic mail applications brought the management of these corporate resources under the umbrella of the information resources management concept. In the early 1980s, these functions were consolidated in most organizations at the senior management level -- at the same level of importance as personnel, marketing, and financial management.

B. Corporate Information Management (CIM) in the 1990's

The next stage is beginning to emerge: the information-literate organization stage.[9] The information-literate organization provides an environment in which individuals and groups think in terms of the knowledge they require to deal effectively with their responsibilities and opportunities. Businesses are being forced by global competition to build information-literate organizations. They are literally using information as a weapon in their competition.

In the crisis/emergency management arena, just as in the world of global competition, it is vital that decisionmakers develop a strategic plan for succeeding in the information age! The latest strategic planning concept is called corporate information management or CIM. CIM provides the framework for establishing a strategic vision and for developing the plans to reach this goal. In reaching concensus on these plans, the organization is strengthened by the inter-divisional communication and bonding that takes place.

CIM is a phased process that includes three major activities:

- The Functional Vision
- The Functional Business Plan
- The Information Systems Strategic Plan

* * * * * * * * * * * *

[9] Weber, E. Sue et al Crisis planning Systems: Tools for Intelligent Action (University of Arizona: September 1988)

The functional vision provides the strategic or "futuristic" vision for the business activity or function. It is a functional description of what the particluar business activity will look like in 10 to 20 years. It is written in clear concise statements that all can understand. It is supported by documentation of the mission, functions, and scope of the activity. It includes policy and guidelines for reaching the vision.

The functional business plan contains the requirements for the future and specifies actions that must be taken to provide a transition of the business activity or function from its current state to the desired future state. Both the current and desired future states are developed through a structured decomposition process -- similar to that used by software engineers. The process to define the desired future state is derived from the decomposition of the goals, objectives and strategies developed in the first activity -- functional vision. The functional business plan includes the business activity's functional information systems requirements. These requirements feed the next major activity -- the information systems strategy.

The information systems strategy is the milestones and procedures that will be used to provide a transition of the information systems from their current support of the function to the future business enhancing configuration. The strategy is derived from an analysis of what exists and its functionality to the functionality of what will be required to support the future

requirements. The resultant strategy may range from continuing to use extant information systems to a complete system redesign to meet the consolided support requirements of several business activities. In the case of the need for a multi-year system redesign effort, the strategy would include provision for interim

The goals of the CIM activities are to:

- increase management efficiencies in the several mission areas,
- improve the effective use of information systems
- reduce duplicative systems supporting the same functional requirements

The key objectives of CIM are:

- implement a systematic way of doing business,
- achieve quality and consistency of information,
- reduce the cost of supporting the information systems infrastructure,
- produce standard functional requirements, and
- migrate toward standard systems for supporting the requirements.

The CIM process usually begins with the development of functional groups to examine a particular business activity from top to bottom. The functional groups have the following major objectives:

- develop a vision of the desired future function;
- review, evaluate, and if necessary, revise the the business policies, practices and procedures of the functional area;

- develop the information systems requirements for supporting the functional area; and,
- define the standard and consistent functional requirements for which standard, integrated information systems can be developed.

The degree of leadership and high-level participation in the overall CIM process and in each of the functional groups is key to the development of a common and clear vision for the future business activity. It is also key to development of consistant policies, practices, and cost-effective supporting information systems.

Conversations with personnel from the Department of Defense, Corporate Information Management Office, indicate that the initial functional groups have developed a team cohesion-- a cohesion that has been developed by the sharing of information between elements (the different services). This by-product of CIM alone may justify the effort.

In some cases refinements to the business methods result from re-thinking the process; in this case, the refinement doesn't involve information systems at all. In many cases, by putting their heads together, the groups have discovered better, more efficient ways of doing business. For example, group members may find that by one organization giving up on a seldom used feature, everyone can enjoy a common information system. Quite often an information technologist in a CIM group may suggest a way to use information systems to revolutionize the way business is done.

Why is the CIO a prerequisite to CIM? There are three primary reasons. First the CIM process is very structured. The CIO grew up in a structured environment. He most likely had a hand in developing the structured software tools that are now used by software engineers. Second, the CIM process must consider information systems requirements and capabilities at each step, if functional requirements and their supporting and evolving information system capabilities are to dovetail at a future point in time. As you will find out in the next chapter, the CIO knows the business and he knows the technology; he acts as a bridge. Third, quite often the CIO and his supporting information technologists are able to suggest an informations systems approach to improve the business. The CIO is needed to insure these suggestions get proper consideration at the highest levels of the organization.

This is where FEMA can seize the initiative: applying the principle of CIM to crisis/emergency management. FEMA can posture itself for the coming of the information age! This is a case where being small (lean and mean) is an advantage. It means FEMA can reorganize its information systems under the leadership of a CIO and begin to implement CIM; and, thereby establish itself in the leadership position in national emergency management.

C. Technologies of the 1990's

The paragraphs that follow describe extant and emerging technologies that are representative of capabilities that must be considered in crisis/emergency management business planning for the information age. These are the kinds of information systems technologies that may give FEMA competitive advantage over other participants in the emergency management community. By using these kinds of technologies, the life-saving response to emergencies will be swift and effective. They will bring valuable new information sources and capabilities to bear on emergencies.

1. Aerial Reconnaissance and Photo Interpretation

Aerial reconnaissance is applicable to each phase of crisis /emergency management. It can benefit the preparedness phase by documenting the past and present. Documenting the past gives a baseline on which to judge the present -- looking for potential hazards. For example, one could see where toxic waste sites have been covered over with modern construction or where homes have been built in a flood-prone area.

Aerial photography can also help crisis/emergency managers in their mitigation efforts. For example, hydrologists using photography can predict the runoff from snow melt in the Spring in the Rocky Mountains. Using this information, water levels behind downstream dams can be lowered in anticipation of the heavy Spring

runoff to alleviate the danger. Residents can be warned.

In the response and recovery phases, aerial photography can save lives and property and speed recovery by providing a quick damage assessment. This damage assessment can pinpoint areas for the initial focus. For example, it could note an oil spill headed for the water intake of a municipal water treatment facility and direct response efforts there.

2. Public Information and Emergency Broadcast

In this day of increasing technical complexity, the potential for hazardous material spills, the release of toxic gases into the atmosphere, etc., it is imperative that we have in place a viable public information and emergency broadcast system. Since the onset of the Persian Gulf war, we have all marveled at the operation of the Saudi Arabian and Israeli systems that warned of incoming Iraqi Scud Missiles. In contrast, we noted with alarm the lack of adequate warning in the Soviet crisis at Chernobyl and the Bhopal toxic chemical emergency. Readily available radio and satellite technology is available to build a reliable sensing and warning system.

3. Geographic Emergency Information System

The demand for improved geographic information and analysis to support crisis/emergency management decisions has grown at a rapid rate. The complexity of potentially hazardous technologies, the scope of modern economic and social systems, and the mobility

of people and materials necessitate a geographic analysis that is national in scope, yet local in detail.[10]

The uncertain location of potential storms, earthquakes, or hazardous spills requires detailed information for the entire nation. The tendency has been for the Federal government to focus on a macro-look at the nation with respect to crisis and to rely on the state and local governments for the details. Unfortunately, when disaster strikes, the Federal analysis is too general and the State and local information either unavailable or in an incompatible format. Often there are inconsistencies in the information that add to the confusion. As Mr. Dobson points out in his article, "It is clear that the Nation would benefit greatly from the installation of a GIS that could be accessed by emergency managers at all levels of government."

The system should be hierarchical in design to permit software and information to be distributed downward from Federal to Federal Region to State Area to County and on to local. Details would be added at the lower levels in a reverse flow to the top.

The Pennsylvania Emergency Management Agency (PEMA) has fielded a spatially-based geographic information system that seems to meet most of the emergency GIS requirements. It provides a geographic-based framework which will facilitate additional

* * * * * * * * * * * *

[10] Dobson, Jerome E. "Geographic Information Systems for Emergency Management" Strategies and Systems for Disaster Survival (Research Alternatives, Inc., Rockville, Maryland: 1988)

capabilities. This system, called the Emergency Information System is marketed commercially by Research Alternatives, Inc. of Rockville, Maryland. The system operates on a IBM compatible Personal Computer -- a definite plus for proliferating an emergency support system. It is in operation in 27 States and is, therefore, well on its way to becoming a de facto standard in the crisis/emergency management community.

4. Information System Highway

An essential ingredient of a National Geographic Emergency Information System is high bandwidth communications between the elements of the emergency response community and the site of a crisis or disaster.

The Federal government is considering the development of an information systems highway or information utility to interconnect DOD contractors and universities nationwide. It seems that the requirements to transmit voluminous emergency management information between respondents could be met by piggybacking on this development. Mobile or portable satellite or microwave radio equipment could connect a disaster site with this information system infrastructure.

5. Portable Radio-Telephone

The after action reports from each national disaster bemoan the lack of communications at the scene of the disaster and request the development and proliferation of a cellular-like

radio system. Such a system would require a high bandwidth satellite terminal to connect the cellular system with the surviving infrastructure. A system of this type is technically feasible and relatively inexpensive to acquire and operate. Special arrangements would be required in most locations to share frequencies with commercial carriers. An alternative competing technology is being developed by Motorola Corporation. The system, called Lithium, will use compact radio telephones and a constellation of 77 low orbit satellites to offer worldwide service. It is designed to overcome the problems of existing cellular radio telephones: continuous coverage on long trips and service in remote areas.

Chapter III. Chief Information Officer

A. Concept

Have you ever thought of using information as a weapon? Well, several corporations and government organizations have. Like any new weapons system, the surprise introduction of the information weapon has overwhelmed the enemy. Corporations with forward-looking strategies have used information as a weapon to win business battles over corporations with traditional approaches to business.

Who leads the development of these new weapons systems? Who commanded their use on the field of battle? The Chief Information Officer is the answer to both questions.

What is the force structure concept used to deploy this new weapon system? Victorious corporations have created an integrated force for implementing their organizational, business, and information technology strategies -- under the strong leadership of a Corporate Chief Information Officer.

What are the qualities of the Chief Information Officer? The CIO is a person of vision. and even more importantly, had the vision in time to anticipate the required information -- in fact, so long ago that he could develop and implement a strategy in time to respond to today's needs.

Does the CIO have other special qualities? Yes, he has the executive skills to develop and market this information weapon strategy to the board of directors. He also has the unyielding determination of a marine field commander charged to "take that hill" -- to see his strategy through to implementation. The CIO combines an excellent feel for the business and technology with the "killer" instinct in devising a vision of the decisive new information weapon. The CIO instinctively knows how to "get the right information in the right person's hands the right time to make the right decision"[11] -- what technology to apply to each facet of the business to overwhelm the competition with a future surprise attack.

B. Roles and Responsibilities

What role does the CIO play on the board of directors? The CIO plays a leadership role in the development of the corporate business strategy. He conceives new business ideas -- based on his thorough knowledge of the information resources and technology -- that are often integral to the formulation of the corporate business strategy. To most on the board he seems omniscient: He knows the business. He knows the competition. He knows what others on the board don't -- he knows the information systems technology.

In the technical aspects of the information systems side of the business, he plays a major role in strategic planning, a

* * * * * * * * * * * * *

[11] Harris, Catherine L., "Information Power, p. 110 (Business Week, No. 2916, October 16, 1985).

prominent role in long-range planning, and approves medium- and short-range planning. Additionally, he sets objectives for the information systems management component of the corporate strategy.

In the pages that ensue, I describe the many roles and responsibilities of the CIO. As you can see from the enumeration that follows, these roles dovetail with the needs of the corporate information management process. Each role is a key ingredient of effective crisis/emergency management.

- Business partner
- Strategist
- Policy maker
- Agent for change
- Provider and user of information systems
- Crisis/emergency management support
- Other responsibilities

1. Business Partner

As one of the most valuable members of the board of directors, the CIO is an entrepreneur -- assuming the risks and the rewards of the organization for formulation of the strategy to accomplish the organizational goals. He does not just work for the company, he is a business partner. He is a decision maker and a problem solver in all aspects of the business. He is a linchpin in the planning and in the execution of the corporate goals.

He is responsible for the effective and efficient flow of information within the company. He exercises his authority to open new channels of information -- i.e., to bridge the seams of the organization. He promotes cooperation and coordination. When accused of infringing on the turf of another organization, he is able to resolve the conflict quickly by demonstrating how corporate information systems help everyone do a better job and, more importantly, how information systems contribute to the success of the corporation. Information systems are interdivisional in nature and must bridge the organizational boundaries -- if not glue the seams together.

2. Strategist

What is his role in long-range planning? The CIO oversees the development of the multi-year (5 to 10 year) plan for implementing the corporate strategy. This plan presents the area of focus and projects the resource requirements. It portrays alternative configurations -- e.g., replacement of a network of distributed minicomputers with a local area network/wide area network. Organizational and budget implications of each alternative are an important part of the long range plan. The CIO ensures that each alternative is thoroughly analyzed and that the resultant information system strategy is sound.

3. Policy Maker

The CIO sets policy regarding the utilization of information resources within the organization. Policy making is inherent in any job at this level but the CIO must be a policy maker extraordinaire.

The interrelationships between information and such internal and external interests as telecommunications, data processing, privacy and security issues, new products and services, and the realization of the organizational vision demand informations systems policy. How the company handles information resources determines -- in a significant way-- the quality of the decisions, the efficiency of the organization, and the quality of its products and services.

Since information resources are valuable and vital corporate assets, promulgation of an information security (INFOSEC) policy regarding their creation and use is an organizational imperative. The protection of information resources, while a direct concern of the CIO in the development of policy, should be the concern of everyone in the organization. The CIO must keep the concern for the safeguarding of vital resources at the forefront of the entire organization.

At the height of a crisis, particularly a crisis after a crisis, it is difficult to adhere to the organizational safeguarding policy. However, this may be the most important time

for adhering to this policy. Information vital to an important decision may become unavailable as input to a mission-critical decision due to carelessness or equipment failure.

The acquisition of information resources is an important area of policy formulation. It is essential that the CIO develop an acquisition policy that encourages interdivisional coordination of (joint) acquisitions in the interest of economies of scale, standardization, and interoperability.

Life cycle management is a major feature of an effective acquisition policy. In the Federal Government, the Office of Management and Budget, Circular A-109, provides mandatory guidance for the acquisition and life cycle management of major systems. (Major systems are defined as those that cost over $100,000,000.) In the government, the CIO is a champion of Government-wide policy guidance.

It is not my intent to suggest the CIO should be an information systems czar, but it is important that he have the authority to bring together these important corporate resources so that it may accomplish its mission and strategic goals.

Another important area of policy is for information dissemination. The success of an organization depends on the effective and efficient communication of information. Effective dissemination calls for adherence to exacting data and protocol standards. In a crisis, where the exact circumstances have never before been encountered, adherence to standards may be

especially important -- else valuable time will be consumed in conversion, or perhaps information will remain unintelligible. Pre-positioning and maintenance are important to this policy.

The CIO must address the availability and access of information in the development of policy. In a crisis, policy in this regard is especially important owing to both the importance of information to the decision makers and to the fact that, usually, some aspect of the vital information is sensitive, classified, or proprietary. The best means to share these data is vitally important. Details of these sharing arrangements can't wait until the crisis unfolds and the information service is needed. For example, the pre-coordination of radio frequencies, protocols, call signs, and cryptographic keys may be the difference between success and failure.

All CIO policy statements should encourage the use of information. For unless employees are stimulated to share and coordinate the use of information, productivity will lag and profits will diminish. Successful resolution of a crisis depends on having worked out the quirks, incompatibilities, or details of the information systems in day-to-day use. This argues strongly for an integrated systems development approach followed by an exhaustive test and evaluation program..

4. Agent for Change

In his role as an agent for change, the CIO must have access to sufficient personnel and capital resources to accomplish

the corporate goals and objectives.

The nature of today's crises and emergencies requires that the CIO have the perspicuity (almost to the point of clairvoyance) to plan for the evolution of information systems and information resources in the required direction -- usually in the direction of greater flexibility and ease of use.

With his knowledge of information technology, the CIO must spearhead the implementation of more capable systems, making sure that redundancy and fault tolerance and other capabilities for coping with a crisis are included in the design. Some organizations, like FEMA, are required to deal with crises and emergencies as a mission. For example, when Hurricane Hugo struck St. Croix in the Virgin Islands, FEMA was fortunate to have had the forethought to acquire a Mobile Air-Transportable Telecommunications System. By contrast, at the onset of Three Mile Island Nuclear Power Plant disaster, FEMA and the other emergency respondents were handicapped by the lack of emergency communications to circumvent the overloaded public telephone system. Also at Three Mile Island, the nuclear emergency response community was slowed because it didn't have remote access to the exact status of the nuclear reactor core.

As one who is involved in one of the most dynamic industries in the world and in one of the most demanding environments -- crisis/emergency management -- the CIO must take the initiative in incorporating the latest technologies and acquiring the necessary resources to ensure the corporation

remains competitive.

In preparation for coping with a crisis, the CIO has the responsibility to have the best available technology. He must have in place anything that will contribute to effective crisis management and the restoration of normal operations. But above all he must have the responsibility to have a recovery capability that is reliable and integrated with the decision-making process.

In crisis/emergency response, where different departments and agencies respond -- depending on the scenario and the level of the participants -- ease of use and training are imperatives. Information must be displayed in a format that is understandable -- and exactly like what they had back in the office. In this regard, the CIO may have to deal with the conflict between the use of de facto standards -- because of their greater popularity -- and Federal acquisition regulations that favor fair and open competition. He must act as a proponent of open systems and other standard interfaces which facilitate access to information.

5. Provider and User of Information Systems

The CIO is both a provider and a user of information. As a provider he must develop information systems and information resources that will enable the corporation or organization to grow and prosper. He must be responsive to the entire user community. The success of the organization depends on his skill at meeting competing demands for service. Here once again, he must balance day-to-day demands with planning and provide for the needs of

crisis managers. He must be aware of the internal needs of the organization -- those that make the corporation run smoothly -- and external needs. In the Federal government, external concerns include the President, Congress, State and local governments, and the public.

In times of crisis or emergency, these latter external needs surface. The presentation of timely information is often responsible for the after-the-fact perception of competence or incompetence of those managing a crisis. In essence, in a crisis, the CIO can provide information that becomes a vehicle for "snatching victory from the jaws of defeat."

Old-line thinking restricts information processing to; acquisition, maintenance, and distribution. The CIO realizes the importance of synthesis, analysis, evaluation, and display in producing new information. This continuous processing, distribution and display acts as seed for value-added information services. When a crisis occurs, the organizations that have continuously refined their information processing system are likely to be responsive to the crisis decision makers. The CIO is responsible for institutionalizing this modernization process.

6. Crisis Management Support

One of the most important, but probably the least appreciated, responsibilities of the CIO is to provide a wide range of support to crisis management. As mentioned above, the

CIO can be instrumental in "snatching victory from the jaws of defeat" by advanced planning for the information needs of a crisis. However, his responsibilities extend beyond this to:

- Develop a cadre of technical specialists who can move, relocate, cannibalize, set-up, and use -- whatever is necessary -- information systems to support the crisis at hand.

- Create an "esprit de corps" and a climate for innovation in the organization to deal with chaotic events.

- Establish an objective crisis "after action" assessment program to evaluate the level of support provided, and create a "remedial action" program to correct any shortcomings in the support.

- Foster cooperative relationships with others, organizations in the government and industry to contact in times of crisis. Generally, people are willing to help respond to a crisis or emergency. The CIO is most valuable in having high-level contacts with the where-with-all and the know-how to help.

- Lead the application of new technology such as expert systems, decision support systems, and geographic informations systems to crisis resolution. Often the crisis managers are not receptive to new technology or departures from familiar ground. The CIO must,

therefore, develop a process for controlled introduction of new developments. By using new techniques, like rapid prototyping, the CIO makes the user a part of the development team.

7. Other Roles and Responsibilities

The CIO is a mover and a shaker. He views information resources and technology from a broad corporate context. He is in full control of the technology of the organization. He integrates computers, communications and information resource management with the business methods and processes for the accomplishment of the corporate vision and strategy. He sponsors knowledge transfer, technical education and research and development -- sufficient to keep his organization on the competitive edge. He prioritizes all technical efforts; he allocates resources to crisis mitigation and response.

C. Some Existing Applications of the CIO Concept

The CIO concept is interesting enough to warrant the issuance of a monthly magazine by IBG Communications Publishers: CIO -- the Magazine for Information Executives. The following excerpts from magazine articles suggest the potential for successes in creating a CIO position in the organization and the possible role(s) of the CIO in crisis/emergency management.

CIOs who don't start boning up on their Eurosystems risk weakening their companies' competitive capability.[12] According to Charles Fitts in an article for CIO magazine, companies doing business in Europe after 1992 will be confronted with new market structures and consumer buying patterns -- and therefore, new problems. But there will be new opportunities as well. Products will have to satisfy only a single European Community (EC) standard instead of conforming to many and conflicting national codes. Most of the red tape associated with commerce in the EC will be reduced.

These changes will have a major impact on the organizational structure and the marketing and distribution strategies of any company doing business in the EC. CIOs will have to develop new systems portfolios to support these new strategic directions. This will require a total rethinking of how information technology can be used in this new competitive environment. In an analogous way, the crisis/emergency management CIO needs to be thinking about the best methods of integrating national assets in support of crises and emergencies.

Today's CIO faces the daunting challenge of splicing information systems (IS) and telecommunications into a solid team.[13] In another article for CIO Magazine, Paul Konstadt describes the merging of two disciplines at Westinghouse Communications, a division of Westinghouse Corporation in

* * * * * * * * * * * *

12 Fitts, Charles "Parlez Vous '92?" (CIO Magazine: May 1990)

13 Konstadt, Paul "Matching a Pair" (CIO Magazine:May 1990).

Pittsburgh. Westinghouse Communications first linked their nationwide business units together via a voice/data digital network, then leased unused portions of the network facilities to defray costs. Reportedly, about half of the traffic on the network now comes from these outside customers. The cost per unit of data transferred is about one-half the cost in 1982. These lowered costs were the result of the strategy to integrate all the business on a voice/data network and to sublease network services to realize the economies of leasing bulk trunks.

According to David Edison, the Westinghouse Communications vice president being interviewed, the blending of the two groups into a single cohesive unit was a textbook case in managerial basics: listening to everyone, building consensus, spending time on team issues, etc. The bottom-up approach worked. Human resources, released by merging IS and telecommunications activities, were used to staff necessary engineering positions. The crisis/emergency management CIO can bring similar benefits to fruition.

The San Francisco earthquake of 1989 provided the first real-life test of the efficacy of commercial disaster recovery services in a widespread disaster. Charles Schwab & Co. Inc. was one of eight clients of Comdisco Disaster Recovery Services Inc. to need help following the earthquake.[14] Because of the uncertainties associated with earthquake predictions, the Schwab planning team realized they needed a plan that could be adapted to

* * * * * * * * * * * *

[14] Melymuka, Kathleen "Gimme Shelter" (CIO Magazine: April 1990)

a wide variety of circumstances. It was a good thing they did. The airport was unexpectedly open. Bridges that were forecast to be open were closed and vice versa. A standby power system failed. Plant personnel overloaded the few available telephone lines to check on their families. The article emphasized the need to exercise backup procedures and arrangements. It also stressed the importance of working with the vendors to make sure they know the organization's recovery plans and can interface with them. In a similar way, the crisis/emergency management CIO must build survivability into national crisis/emergency support systems.

In "The IT Visionaries," Amy Bemar indicates the CIOs share the ability not only to envision strategic uses of information technology (IT), but to garner support and implement winning systems.[15] Amy Bemar reports that each year, a handful of information professionals risk their careers and, often millions of dollars in corporate assets investing in strategic programs designed to position their companies for the future. The American Management Systems,Inc. and Carnegie Mellon University's School of Industrial Administration co-sponsored five awards for Achievements in Managing Information Technology. Her article details accomplishments of these five award recipients.

Jane E. Bailey, Director of Information Systems, Commonwealth of Virginia, Department of Taxation, led an eight-year effort to speed-up the processing of tax returns and corporate tax reporting. This has saved the state over $77

* * * * * * * * * * * *

15 Bemar, Amy "The IT Visionaries" (CIO magazine: December 1989)

million since its inception in 1983. A similar infusion of information technology into emergency operations could be used to speed financial aid to disaster victims.

Bill Eaton, Senior vice president and CIO, Levi Strauss & CO. was instrumental in the development of a network that links retail customers to a merchandise data base that allows Levi Strauss to re-order fast moving items and thus capitalize on a short selling season. The CIO for crisis/emergency management could oversee the development of systems to identify the priority needs for disaster relief amd recovery and to dispatch aid to those in need.

Paul F. Glaser, Chairman Technology Committee, Citicorp's chief technologist, envisioned an era when automated teller machines would revolutionize how banks conducted business. He convinced his corporation to spend millions on their development. He was right! The CIO for crisis/emergency management will need to "risk his reputation" on a few high pay-off information systems. A public information and warning system may be an example of a capability which will need this kind of courage to initiate and get others to support.

James C. Grant, Executive vice president, Systems and Technology, The Royal Bank of Montreal, Canada, conceived an unusual experiment -- that payed off for his bank. He cross-trained the technology and the business divisions. He cultivated a cadre of bankers who knew technology and technologists who knew banking. Bank customers can avail

themselves of over 300 distinct products and services. Today the bank has over $110 billion (Canadian) in assets and holds a significant lead over other national banks in the country. Training which fuses business methods and information technology is an especially important responsibility for the crisis/emergency management CIO. Equivalent advantages are possible through the application of information systems to emergency support.

****

One can see from the above examples some of the benefits which can result from adopting the CIO concept. The examples confirm the roles and responsibilities that have been assigned to the CIO for the business world. They suggest parallel benefits in the development and operation of a nationwide crisis/emergency response system.

Chapter IV. Conclusion:

This paper identifies three major roles for the CIO for improving national crisis/emergency management response -- especially in the environment of the 21st Century where the response to situational complexities will place increased emphasis on knowledge-based information system solutions. The roles I have identified are:

- The CIO and Corporate Information Management
- The CIO and Information Systems Management
- The CIO and Crisis and Emergency management

The role of the crisis/emergency management CIO is consistent with that identified with forward-looking organizations while the other two roles are a logical extension of the CIM process and the need to use modern technology in response to crises and emergencies.

In the concluding chapter of his book, The Business Value of Computers, Paul A. Strassman presents a "Policy Checklist" for the chief executive officer to use to insure that information resources are being effectively incorporated into the business. The essence of his checklist ideas can be used to tie together the three major roles of the CIO in improving the business of crisis/ emergency management. See the diagram which follows. The picture of nested improvement plans that make up the essential elements of CIM shows information technology at the core. The CIO is important to each level of the nest and, therefore, he is the linchpin for business success. In the case of the business of

crisis/emergency management -- where the gravity of information-dependent decisions could range from life-saving to life-threatening -- the value of the CIO is incalculable.

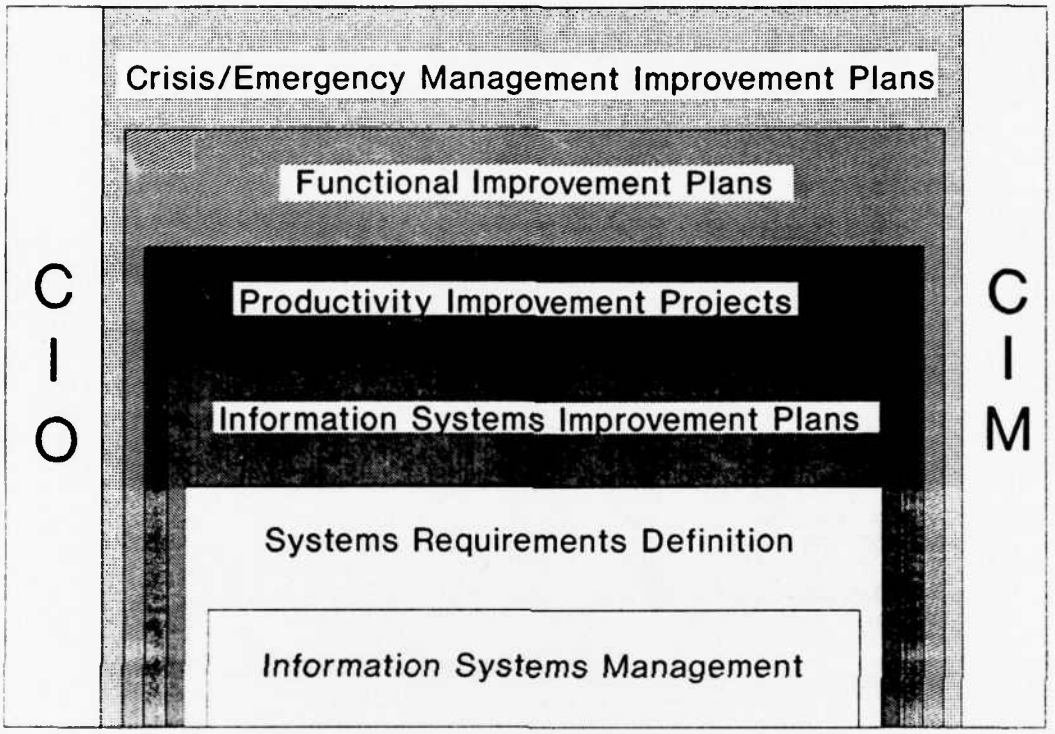

Figure 3. Relating CIO, CIM and Information Systems

A. The CIO and CIM

The crisis/emergency management CIO plays a key role in CIM. CIM provides a planning framework for establishing a strategic vision for the organization, then developing the strategic business and information systems plans to realize this vision. In a parallel track, the CIM provides the framework for

devising tactical plans to sustain business operations while the strategic plans bear fruit. The tactical business and information systems plans are designed to mesh with their strategic counterparts. In a third parallel track, the CIM framework encourages information systems plans to dovetail with both the strategic and tactical business plans.

Existing and evolving information systems technologies are considered at each step in the CIM process. At times, difficult, yet strategically important decisions must be made. Should the organization follow a high-technology/high-risk path or continue with a lower-risk manual approach? A decision of this type may be pivotal in determining the success or failure of the organization in a future crisis or emergency situation. The CIO, with his combined business and information systems acumen, is most likely to recognize the true gravity of the decision and to elevate the decision, if necessary, to the board of directors for consideration.

By way of example, consider the importance of the decision to reprogram the Patriot Anti-Aircraft Missile to intercept ballistic missiles on limiting the involvement of Israel in the Persian Gulf War. Equally crucial and difficult would be a decision required to resolve the issue of the requirement for information security (INFOSEC) measures in disaster communications systems. In most national security crises the need is obvious. In most disaster scenarios there is no need. However, for dual use purposes (disaster emergencies and national security crises), one would have to include the information security measures. The

advice of the CIO might be the deciding factor in this issue. He might reason that the cost advantage of a shared system would out-weigh the cumbersomeness of the measures. In a future nuclear weapon accident, the value of this choice would be realized.

The CIO also plays a key leadership role in the development of both CIM strategic and tactical information systems plans. He is responsible for meeting the requirements which result from the CIM corporate business model. Owing to the potential importance of the information systems strategy on the future success of the organization, the strategy needs a proponent -- of equal stature as the business-area managers -- on the board of directors to defend the information system priorities and to secure the implementing resources.

B. The CIO and Information Systems

In addition to his role as a linchpin in CIM, the CIO has a more traditional but equally important role to play in information systems management. Here, the CIO directs an intelligent organization: "Functioning as both highway engineers and state troopers on our fast growing electronic highways -- they build as well as manage the systems - - they are put in the distasteful position of being, in a sense, the corporation's "executive

thought police".[16]

The CIO and his intelligent organization must be capable of evolving an effective crisis/emergency planning, training, and support system. The CIO and his intelligent organization must be inclined to evolutionary developments. They must start with a well-designed architecture. Since most decision makers served by the CIO and his organization are skeptical of modern technology, they must be nurtured at first. The system must adapt to a variety of management styles.

The development and the implementation of information systems technology must follow the "build-a-little, test-a-little, build-a-little more" principle of "rapid prototyping," which involves the users (decision makers) in each step of system development and permits the system to grow in sophistication. This approach is doubly important in the development of a crisis/emergency management system, if it is to be effectively used under duress.

The CIO is the source of technical innovation and service delivery. Here, he must insure that the technologists who work for him are listening and responding to the users' requirements. Developments need to involve the users at each step if they are to be acceptable. His organization must always have something new in the pipeline to meet user demands for service. He knows as users

* * * * * * * * * * * *

16 Toffler, Alvin "The Executive Thought Police" (Powershift: Knowledge, Wealth, and Violence at the Edge of the 21th Century, November 1990)

become more knowledgeable about informations systems, they demand better services. The information systems organization must stay several steps ahead of the user in understanding new technology.

The CIO and his organization must aggressively reduce the cost while improving the performance of services. In this role the CIO must know the total life cycle costs associated with the various technologies and service alternatives.

The CIO must be an agent for change. He must actively pursue resolution of the users' problems and concerns. He must be creative in the acquisition of new technology. Long acquisition cycles and state-of-the-art information systems services are contradictory.

The CIO must work effectively across all functional areas of the organization. He must be an unbiased leader who champions the "right" solution. Often, the CIO will have to take an unpopular stance. For example, he may have to sponsor an open systems approach in opposition to a major business-area leader in the interest of standardization and long-term benefits. The CIO must "work the seams" between the various functional areas.

The CIO must be a champion of state-of-the-art concepts. He must diligently shed the old images of "ADP shops operating behind closed doors," or of " a roll of quarters and a telephone booth" telecommunications. He must espouse the virtues of the possibilities and advantages of "rule-based systems," "intelligent organizations," "local area networks/wide area

networks," etc. Additionally, in crisis/emergency management, he must champion the technologies of the 1990's like those mentioned in this paper.

C. The CIO and Crisis/Emergency Management

The CIO plays a more crucial role in the business of crisis/emergency management than the role other CIOs play in their organizations due to the impact of his leadership on saving lives and relieving the anxieties in the wake of disasters. In this role the CIO is instrumental in the following ways:

- He assists the entire organization in the use of CIM to develop a systematic way of responding to the several functions of crisis/emergency management. See pages 13-15.

- He oversees the development and operation of supporting information systems.

- He develops scenario-driven responses to the full range of foreseeable crises and emergencies.

- He manages, often through a network of inter-personal relationships, a "ROLODEX" of available information systems capabilities which he can summon should the

situation demand an unusual response.

- He creates and manages an innovative work environment. He calls on his staff to perform miracles to meet the uncertainties of crises and emergencies. In the Persian Gulf War, Defense Communication Agency innovators were able to change the orbit of an old military satellite to provide additional circuit capacity. This kind of creativity is needed to effect support in catastrophic situations.

- Above all, the CIO must be an authority figure. He must be able to mastermind and oversee the development of a national crisis/emergency management system. This development must pull together the disparate assets of Federal, State and local governments and, in some cases, private industry. Here, using an approach similar to that used by General H. Norman Schwarzkopf and his staff to build a battlefield coalition in the Persian Gulf War, the CIO must mastermind an operational coalition of the emergency response community. The stature of the CIO will be key to securing the support and cooperation needed to bring about the required integration.

In summary, this paper identifies three key roles for the CIO in the development and maintenance of a national crisis/emergency management system -- roles that not only fulfill the vision of FEMA's creators but also realize the vision of the new FEMA Director, Mr. Wallace E. Stickney in his interview for the Journal of Civil Defense, February 1991 issue. (See his quote at the front of this paper.)

Bibliography

Bemar, Amy "The IT Visionaries," CIO Magazine (December 1989).

Carter, Jimmy "Message form the President" The White House Conference on Library and Information Service (Conference Program: November 15-19, 1979).

Dobson, Jerome E. "Geographic Information Systems for Emergency Management" Strategies and Systems for Disaster Survival (Research Alternatives, Inc., Rockville, Maryland: 1988).

Executive Order 12656 Assignment of Emergency Preparedness Responsibilities.

Fitts, Charles "Parlez Vous '92?" CIO Magazine (May 1990).

Harris, Catherine L., "Information Power," p. 110 Business Week, No. 2916, (October 16, 1985).

Konstadt, Paul "Matching a Pair" CIO Magazine (May 1990).

Mann, Nancy R., "Today -- The Japanese Challenge and the Fourteen Points" The Keys to Excellence: The Story of The Demming Philosophy, pp. 43-45 (Prestwick Books, Los Angeles: 1988)

Mathews, Jay and Peterson, Cass "Oil Tanker Captain Fired After Failing Alcohol Test: Exxon Blames Government for Cleanup Delay" The Washington Post, pp. A1&A6 (The Washington Post Company: March 31, 1989).

Mathews, Jay "In Alaska, Oil Spill has lost Its Sheen" The Washington Post (The Washington Post: February 9, 1991).

Melymuka, Kathleen "Gimme Shelter" CIO Magazine (April 1990).

Morentz, James W. "Operating with Information Systems During an Emergency" Strategies and Systems for Disaster Survival (Research Alternatives Inc.: Rockville, Maryland 1988).

Morentz, James W. Interview with President of Research Alternatives, Inc.(Rockville, Maryland: February 4, 1991).

Phillips, Warren R. and Rimkunas, Richard Crisis Warning, pp. 2-3 (Gordon and Breach Science Publishers, New York: 1983).

Public Affairs, Office of Assistant Secretary of Defense "Pentagon Adopts Plan for Corporate Information Management" (News Release No. 50-91, January 29, 1991).

Smith, Charles A.P. Decision Making Under Time Pressure: The Effects of Time Pressure on Information Search Strategy, Decision Strategy, Consistency, and Outcome Quality (University of Arizona: 1990).

Stickney, Wallace E. "Meet Wallace E. Stickney -- New FEMA Director" Journal of Civil Defense (American Civil Defense Association: February 1991).

Toffler, Alvin "The Executive Thought Police" Powershift: Knowledge, Wealth, and Violence at the Edge of the 21th Century, (Bantam Books: New York, November 1990).

Weber, E. Sue et al Crisis planning Systems: Tools for Intelligent Action (University of Arizona: September 1988).